Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 14 (2008) 59–64

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Exponential sums for nonlinear recurring sequences

Harald Niederreiter [a], Arne Winterhof [b,*]

[a] *Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore*

[b] *Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenberger Straße 69, A-4040 Linz, Austria*

Received 7 March 2006

Available online 1 November 2006

Communicated by Stephen D. Cohen

Dedicated to Igor Shparlinski on the occasion of his 50th birthday

Abstract

We prove a new bound on exponential sums for nonlinear recurring sequences. This result improves on an earlier bound of Niederreiter and Shparlinski. An application to the distribution and statistical independence of nonlinear congruential pseudorandom numbers is given.

Keywords: Exponential sums; Recurring sequences; Pseudorandom numbers; Discrepancy

1. Introduction

For a prime p we identify the finite field $\mathbb{F}_p$ of p elements with the set of integers $\{0, 1, \ldots, p-1\}$. Let $f(X)$ be a polynomial over $\mathbb{F}_p$ of degree $d \geqslant 2$ and (u_n) the sequence of elements of $\mathbb{F}_p$ obtained by the recurrence relation

$$u_{n+1} = f(u_n), \quad n \geqslant 0, \tag{1}$$

with some initial value u_0. Obviously, this sequence eventually becomes periodic with least period $t \leqslant p$, but we restrict ourselves to the case where (u_n) is purely periodic.

* Corresponding author.
E-mail addresses: nied@math.nus.edu.sg (H. Niederreiter), arne.winterhof@oeaw.ac.at (A. Winterhof).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2006.09.010

We consider the incomplete exponential sums

$$S(a_0,\ldots,a_{s-1};N)=\sum_{n=0}^{N-1}\mathrm{e}_p\left(\sum_{j=0}^{s-1}a_ju_{n+j}\right),\quad 1\leqslant N\leqslant t,\ s\geqslant 1,$$

where $\mathrm{e}_p(z)=\exp(2\pi iz/p)$ and $a_0,\ldots,a_{s-1}$ are integers that are not all divisible by p. In [10] Niederreiter and Shparlinski proved the bound

$$S(a_0,\ldots,a_{s-1};N)=O\big(N^{1/2}p^{1/2}(\log p)^{-1/2}\big), \tag{2}$$

where the implied constant depends only on d and s. The bound (2) is nontrivial only if N is at least of order of magnitude $p/\log p$. In Section 2 we modify the method of [10] and prove a bound on $S(a_0,\ldots,a_{s-1};N)$ which is nontrivial for N at least of the order of magnitude $p/\psi(p)$ for any function $\psi(p)\geqslant 2$ with $\lim_{p\to\infty}(\log\psi(p))/\log p=0$.

In Section 3 we apply the exponential sum bound to analyse the distribution and statistical independence of *nonlinear congruential pseudorandom numbers* u_n/p, $n\geqslant 0$, in the unit interval in terms of a discrepancy bound. We refer to [9, Chapter 8] and [12] for background on nonlinear congruential pseudorandom numbers.

2. Exponential sum bound

In this section, we improve on the bound (2) by refining the method of bounding exponential sums that was introduced in [10] and [11].

Theorem 1. *If the sequence* (u_n)*, given by* (1) *with a polynomial* $f(X)\in\mathbb{F}_p[X]$ *of degree* $d\geqslant 2$*, is purely periodic with period* t *and* $1\leqslant N\leqslant t$*, then the bound*

$$\max_{\gcd(a_0,\ldots,a_{s-1},p)=1}\big|S(a_0,\ldots,a_{s-1};N)\big|=O\left(N\left(\frac{\log(2p/N)}{\log p}\right)^{1/2}\right)$$

holds, where the implied constant depends only on d *and* s*.*

Proof. We can assume $N\geqslant 2p^{1/2}$, for otherwise the theorem is trivial. We first prove that, for any integer $r\geqslant 1$ and $\gcd(a_0,\ldots,a_{s-1},p)=1$, we have

$$S(a_0,\ldots,a_{s-1};N)=O\big(Nr^{1/2}(p/N)^{1/(2r)}\big(\min\big\{\log p,rp^{1/(10r)}\big\}\big)^{-1/2}\big) \tag{3}$$

for $2p^{1/2}\leqslant N\leqslant t$. Since otherwise (3) is trivial, we may assume $r<\log p$.

It is obvious that for any integer $k\geqslant 0$ we have

$$\left|S(a_0,\ldots,a_{s-1};N)-\sum_{n=0}^{N-1}\mathrm{e}_p\left(\sum_{j=0}^{s-1}a_ju_{n+j+k}\right)\right|\leqslant 2k.$$

Therefore, for any integer $K\geqslant 1$,

$$K\big|S(a_0,\ldots,a_{s-1};N)\big|\leqslant W+K(K-1), \tag{4}$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathrm{e}_p\left(\sum_{j=0}^{s-1} a_j u_{n+j+k} \right) \right|.$$

We consider the sequence of polynomials $f_k(X) \in \mathbb{F}_p[X]$ defined by

$$f_0(X) = X, \qquad f_k(X) = f\big(f_{k-1}(X)\big), \quad k \geqslant 1.$$

By the Hölder inequality, using $u_{n+k} = f_k(u_n)$ and putting

$$F_k(X) = \sum_{j=0}^{s-1} a_j f_{k+j}(X),$$

we obtain

$$\begin{aligned} W^{2r} &\leqslant N^{2r-1} \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathrm{e}_p\big(F_k(u_n)\big) \right|^{2r} \\ &\leqslant N^{2r-1} \sum_{x \in \mathbb{F}_p} \left| \sum_{k=0}^{K-1} \mathrm{e}_p\big(F_k(x)\big) \right|^{2r} \\ &\leqslant N^{2r-1} \sum_{k_1,\ldots,k_{2r}=0}^{K-1} \left| \sum_{x \in \mathbb{F}_p} \mathrm{e}_p\big(F_{k_1,\ldots,k_{2r}}(x)\big) \right|, \end{aligned}$$

where $F_{k_1,\ldots,k_{2r}}(X) = F_{k_1}(X) + \cdots + F_{k_r}(X) - F_{k_{r+1}}(X) - \cdots - F_{k_{2r}}(X)$. If $\{k_1, \ldots, k_r\} = \{k_{r+1}, \ldots, k_{2r}\}$ as multisets, then $F_{k_1,\ldots,k_{2r}}(X)$ is constant and the inner sum is trivially equal to p. There are at most $r!K^r \leqslant r^r K^r$ such sums. Otherwise we can apply Weil's bound (see e.g. [8, Chapter 5]) to the inner sum using $\deg(F_{k_1,\ldots,k_{2r}}) \leqslant d^{K+s-2}$, to get the upper bound $d^{K+s-2} p^{1/2}$ for at most K^{2r} sums. Hence,

$$W^{2r} \leqslant r^r K^r N^{2r-1} p + d^{K+s-2} K^{2r} N^{2r-1} p^{1/2}. \tag{5}$$

Choose

$$K = \min\left\{ \left\lceil 0.4 \frac{\log p}{\log d} \right\rceil, \left\lfloor r p^{1/(10r)} \right\rfloor \right\}.$$

Then it is easy to see that the first term on the right-hand side of (5) dominates the second one in terms of the order of magnitude in p, and we get (3) from (4) and (5) after simple calculations.

Finally, we choose

$$r = \left\lfloor \log(p/N) \right\rfloor + 1.$$

Note that $r < \log p$ since $N \geqslant 2p^{1/2} > e$. If $N > p/e$, then we have $r = 1$ and the theorem follows immediately from (3). If $N \leqslant p/e$, then we have

$$rp^{1/(10r)} \geqslant \log(p/N)e^{0.05(\log p)/\log(p/N)} \geqslant 0.05 \log p$$

and the theorem follows again from (3). □

Corollary 1. *For any function $\psi(p) \geqslant 2$ with*

$$\lim_{p\to\infty} \frac{\log \psi(p)}{\log p} = 0$$

and any $N \geqslant p/\psi(p)$ we have

$$\max_{\gcd(a_0,\ldots,a_{s-1},p)=1} \left|S(a_0,\ldots,a_{s-1};N)\right| = O\left(N\left(\frac{\log \psi(p)}{\log p}\right)^{1/2}\right) = o(N).$$

3. Discrepancy bound

Let (u_n) again be the sequence generated by (1). For a positive integer s, the discrepancy $D_s(N)$ of the N points

$$\left(\frac{u_n}{p},\ldots,\frac{u_{n+s-1}}{p}\right), \quad n = 0, 1, \ldots, N-1, \tag{6}$$

in the half-open unit interval $[0,1)^s$ is defined by

$$D_s(N) = \sup_{B\subseteq[0,1)^s} \left|\frac{N(B)}{N} - V(B)\right|,$$

where $N(B)$ denotes the number of points (6) which hit the box

$$B = [a_1, b_1) \times \cdots \times [a_s, b_s) \subseteq [0,1)^s,$$

the supremum is taken over all such boxes B and $V(B)$ is the volume of B.

The following theorem improves on the discrepancy bound for nonlinear congruential pseudorandom numbers that was established in [10].

Theorem 2. *If the sequence (u_n), given by* (1) *with a polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $d \geqslant 2$, is purely periodic with period $t \geqslant 3$ and $3 \leqslant N \leqslant t$, then the bound*

$$D_s(N) = O\left(\left(\frac{\log(2p/N)}{\log p}\right)^{1/2}\left(\log\frac{\log p}{\log(2p/N)}\right)^{s}\right)$$

holds, where the implied constant depends only on d and s.

Proof. Put

$$H = \left\lceil \left(\frac{\log p}{\log(2p/N)} \right)^{1/2} \right\rceil.$$

Then $1 < H < p$. By the Erdős–Turán–Koksma inequality (see e.g. [2, Theorem 1.21]) we obtain

$$D_s(N) \leqslant C_s \left(\frac{1}{H} + \frac{1}{N} \sum_{0<|\mathbf{a}|\leqslant H} \frac{1}{\rho(\mathbf{a})} \big| S(a_0, \ldots, a_{s-1}; N) \big| \right),$$

where $C_s > 0$ is a constant depending only on s and where for $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$ we put

$$|\mathbf{a}| = \max\big(|a_0|, \ldots, |a_{s-1}|\big),$$
$$\rho(\mathbf{a}) = \prod_{j=0}^{s-1} \max\big(|a_j|, 1\big).$$

Now Theorem 1 yields

$$D_s(N) = O\left(\frac{1}{H} + \left(\frac{\log(2p/N)}{\log p} \right)^{1/2} \sum_{0<|\mathbf{a}|\leqslant H} \frac{1}{\rho(\mathbf{a})} \right)$$
$$= O\left(\frac{1}{H} + \left(\frac{\log(2p/N)}{\log p} \right)^{1/2} (\log H)^s \right)$$

with implied constants depending only on d and s. Using the specific value of H, we arrive at the result of the theorem. □

Corollary 2. *For any function $\psi(p) \geqslant 2$ with*

$$\lim_{p\to\infty} \frac{\log \psi(p)}{\log p} = 0$$

and any $N \geqslant p/\psi(p)$ we have

$$D_s(N) = O\left(\left(\frac{\log \psi(p)}{\log p} \right)^{1/2} \left(\log \frac{\log p}{\log \psi(p)} \right)^s \right) = o(1).$$

4. Remarks

It seems that the approach of this paper may also lead to improvements on the bounds in [3,4,6, 7,13]. The improved method was already used in [5] as well. More precisely, the papers [3,4] deal with nonlinear recurrences $y_{n+1} \equiv f(y_n) \bmod M$ with composite moduli M. The papers [6,7] contain extensions of (2) to nonlinear recurrences of higher orders $y_{n+1} = f(y_n, \ldots, y_{n-m+1})$ for some $m \geqslant 1$ (see also the recent paper [1]). In [5] sequences $y_{n+1} = f(y_n, n)$ are considered. Finally, in [13] we proved analogs of (2) for multiplicative character sums over finite fields for nonlinear recurring sequences and their applications to the distribution of powers and primitive roots in finite fields.

Acknowledgments

The authors thank Igor Shparlinski for useful discussions. The second author was supported by the Austrian Science Fund (FWF) under research grant P19004-N18.

References

[1] S.R. Blackburn, I.E. Shparlinski, Character sums and nonlinear recurrence sequences, Discrete Math. 306 (2006) 1126–1131.
[2] M. Drmota, R.F. Tichy, Sequences, Discrepancies and Applications, Lecture Notes in Math., vol. 1651, Springer, Berlin, 1997.
[3] E.D. El-Mahassni, I.E. Shparlinski, A. Winterhof, Distribution of nonlinear congruential pseudorandom numbers modulo almost squarefree integers, Monatsh. Math. 148 (2006) 297–307.
[4] E.D. El-Mahassni, A. Winterhof, On the distribution of nonlinear congruential pseudorandom numbers in residue rings, Int. J. Number Theory 2 (2006) 163–168.
[5] E.D. El-Mahassni, A. Winterhof, On the distribution and linear complexity of counter-dependent nonlinear congruential pseudorandom number generators, JP J. Algebra Number Theory Appl. 6 (2006) 411–423.
[6] F. Griffin, H. Niederreiter, I.E. Shparlinski, On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Honolulu, HI, 1999, in: Lecture Notes in Comput. Sci., vol. 1719, Springer, Berlin, 1999, pp. 87–93.
[7] J. Gutierrez, D. Gomez-Perez, Iterations of multivariate polynomials and discrepancy of pseudorandom numbers, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Melbourne, 2001, in: Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 192–199.
[8] R. Lidl, H. Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge, 1997.
[9] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, SIAM, Philadelphia, 1992.
[10] H. Niederreiter, I.E. Shparlinski, On the distribution and lattice structure of nonlinear congruential pseudorandom numbers, Finite Fields Appl. 5 (1999) 246–253.
[11] H. Niederreiter, I.E. Shparlinski, On the distribution of inversive congruential pseudorandom numbers in parts of the period, Math. Comp. 70 (2001) 1569–1574.
[12] H. Niederreiter, I.E. Shparlinski, Recent advances in the theory of nonlinear pseudorandom number generators, in: Monte Carlo and Quasi-Monte Carlo Methods 2000, Hong Kong, 2000, Springer, Berlin, 2002, pp. 86–102.
[13] H. Niederreiter, A. Winterhof, Multiplicative character sums for nonlinear recurring sequences, Acta Arith. 111 (2004) 299–305.